

ثغرة حرجية في إضافة ووردبريس CVE-2026-85097 تتعرض للاستغلال نشط



ثغرة أمنية بالغة الخطورة في إضافة Bricksforge لنظام ووردبريس تتعرض للاستغلال النشط، مما يتيح للمهاجمين غير المصادق عليهم تنفيذ أكواد عن بُعد.

- الثغرة CVE-2026-85097 حاصلة على تقييم CVSS بدرجة 10.0، وهي أقصى درجة خطورة
- تؤثر الثغرة على إضافة Bricksforge لمواقع ووردبريس
- يمكن للمهاجمين رفع وتنفيذ أكواد PHP تعسفية دون مصادقة
- أكد باحثو Patchstack وقوع استغلال نشط للثغرة
- تتيح الثغرة تنفيذ أكواد عن بُعد بشكل كامل على المواقع المعرضة للخطر

تفاصيل الثغرة الأمنية

تم تحديد ثغرة أمنية حرجة تحمل الرمز **CVE-2026-85097** في إضافة Bricksforge لنظام ووردبريس، وهي الآن تتعرض لاستغلال نشط. حصلت الثغرة على أقصى تقييم في نظام تقييم الثغرات الأمنية الشائعة (CVSS) بدرجة 10.0، مما يعكس خطورتها البالغة. وفقاً لباحثي الأمن السيبراني في Patchstack، تتيح الثغرة للمهاجمين غير المصادق عليهم رفع وتنفيذ أكواد PHP تعسفية على مواقع ووردبريس المتأثرة.

آلية الهجوم

تمكّن الثغرة من تنفيذ الأكواد عن بُعد (RCE) دون الحاجة لأي شكل من أشكال المصادقة. وهذا يعني أن المهاجمين يمكنهم السيطرة الكاملة على مواقع ووردبريس المعرضة للخطر من خلال استغلال الثغرة لرفع ملفات PHP خبيثة وتنفيذها على الخادم المستهدف. إن طبيعة الاستغلال التي لا تتطلب مصادقة تخفض بشكل كبير حاجز الدخول أمام المهاجمين، حيث لا حاجة لبيانات اعتماد أو وصول مسبق للنظام.

تأكيد الاستغلال النشط

أكدت Patchstack أن الجهات المهددة تستغل هذه الثغرة بنشاط في هجمات حقيقية. تواجه المؤسسات التي تشغل مواقع ووردبريس مع إضافة Bricksforge خطراً فوراً للاختراق، مما قد يؤدي إلى اختراق البيانات أو تشويه المواقع أو توزيع البرمجيات الخبيثة أو استخدام الخوادم المخترقة كنقاط ارتكاز لشن هجمات إضافية داخل البيئات الشبكية.

ما يجب فعله الآن

1. تحديد جميع مواقع ووردبريس ضمن البنية التحتية للمؤسسة فوراً والتحقق من وجود إضافة Bricksforge
2. تعطيل أو إزالة إضافة Bricksforge من جميع مواقع ووردبريس حتى توفر تحديث أمني واختباره
3. مراجعة سجلات خوادم الويب للكشف عن محاولات مشبوهة لرفع أو تنفيذ ملفات PHP تستهدف مواقع ووردبريس
4. تطبيق قواعد جدار حماية تطبيقات الويب (WAF) لحظر محاولات رفع الملفات غير المصادق عليها إلى مجلدات إضافات ووردبريس
5. إجراء تحليل جنائي رقمي لأي مواقع ووردبريس تشغل Bricksforge للكشف عن مؤشرات اختراق محتملة
6. تحديث إجراءات الاستجابة للحوادث لتشمل إدارة ثغرات إضافات ووردبريس والتنسيق مع فرق تطوير الويب بشأن عمليات فحص الإضافات الآمنة